UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/728,520	12/01/2000	Kun Wah Yip	609920600012	5426

7590 05/24/2004

David B. Cochran
Jones, Day, Reavis & Pogue
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	4

DATE MAILED: 05/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/728,520	YIP ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 December 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Pursuant to USC 131, claims 1-35 are presented for examination.

Specification

2. The disclosure is objected to because of the following informalities: on page 14, line 11, there is a typo error on the word "means", page 4, line 12, "electronic is misspelled", page 15, line 14, there is a typo error on the word "retrieving", page 8, line 21 "configuration", etc. just to name a few. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the application.

The disclosure is objected to because of the following informalities: on page 16, line 21, reference number "230" should be --223 --. Appropriate correction is required.

The disclosure is objected to because there is inconsistency with the description of reference number 60 on page 18, lines 19 and 20.

Claim Objections

3. **Claim 7** is objected to because of the following informalities: on line 17, page 22 the word "wherein" is misspelled. Appropriate correction is required.

3.1 **Claims 14 and 29** are objected to because of the following informalities: on page 24, line 23 and page 28, line 21, the word "configuration" is misspelled. The word "overwriting" on the last step of both claims is also misspelled. Appropriate correction is required.

3.2 **Claims 8 and 23** are objected to because of the following informalities: The word "overwriting" on the last step of both claims is also misspelled. Appropriate correction is required.

3.3 **Claim 15** is objected to because of the following informalities: The word "using" on the last step of the claim is also misspelled. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4.1 **Claims 1-5, 15-19, and 30-31** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,385,723 to **Richards**.

4.2 **As per claims 1 and 15, Richards** discloses a method of protecting a configuration data sequence against reverse engineering, wherein the configuration data sequence includes a plurality of configuration bits, and is used to configure the operation of a programmable device, the method comprising the steps of: partially encrypting the configuration bits of the configuration data sequence by altering some, but not all, of the configuration bits, for example (see column 2, lines 58-67); storing the partially-encrypted configuration data sequence in a memory external to the programmable device, for example (see column 4, lines 10-50); storing decryption information for the partially-encrypted configuration data sequence in the programmable device, for example (see column 7, lines 55-67 and column 10, lines 10-18); loading the partially-encrypted configuration data sequence into the programmable device, for example (see column 4, lines 53-60 and column 2, lines 58-67); decrypting the partially-encrypted configuration data sequence using the decryption information stored in the programmable device, for example (see column 11, lines 1-45); and configuring internal logic of the programmable device using the decrypted configuration data sequence, for example (see column 11, line 35 through column 12, line 16).

As per claims 2 and 16, Richards discloses the claimed method of claim 1, wherein the partially-encrypted configuration data sequence is loaded into the programmable device via a wireless connection, for example (see column 4, lines 10-50).

As per claims 3 and 17, Richards discloses the claimed method of claim 1, wherein the decryption information includes a sequence of bits that correspond to the bits of the configuration data sequence, and wherein each bit in the sequence of bits of the decryption information provides an indication of which bits in the configuration data sequence are encrypted, for example (see column 8, line 29 through column 9, line 25).

As per claims 4 and 18, Richards discloses the claimed method of claim 3, wherein the decrypting step further comprises the step of toggling logic values of the bits in the partially-encrypted configuration data sequence that are indicated as being encrypted in the sequence of bits of the decryption information, for example (see column 7, lines 15-31 and column 8, line 40 through column 9, line 25).

As per claims 5 and 19, Richards discloses the claimed method of claim 3, wherein the decrypting step further comprises the step of: modifying logic values of the bits in the partially encrypted data sequence that are indicated as being encrypted in the sequence of bits of the decryption information using a set of logic values stored in the programmable device, for example (see column 7, lines 15-31 and column 8, line 40 through column 9 and column 6, lines 15-56).

As per claim 30, Richards discloses the claimed apparatus of claim 15, wherein the programmable device is a SRAM-based field programmable gate array (FPGA), for example (see column 11, lines 21 through column 12, line 27 and column 1, lines 20-35).

As per claim 31, Richards discloses the claimed apparatus of claim 15, wherein the programmable device is a reconfigurable logic device, for example (see column 11, line 45 through column 12, line 27 and column 1, lines 20-35 and column 4).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.1 **Claims 6-8, 11-14, 20-23, 26-29, 32-35** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,385,723 to **Richards**.

5.2 **As per claim 6, Richards** discloses the claimed method of claim 4, wherein the toggling step further comprises the step of: executing an exclusive-or function between the partially-encrypted configuration data sequence and the sequence of bits of the decryption information, for example (see column 7, lines 15-31 and column 8, line 40 through column 9, line 25). **Richards** discloses using DES algorithm, which includes X-oring function.

As per claims 7 and 22, Richards discloses the claimed method of claim 1, wherein the storing decryption information step further comprises the steps of: storing a first secret sequence in the programmable device, wherein the first secret sequence comprises a sequence of bits that correspond to the bits of the configuration data sequence, and wherein each bit of the first secret sequence provides an indication of which bits in the configuration data sequence are encrypted, for example (see column 8, line 29 through column 9, line 25); and storing a second secret sequence in the programmable device, wherein the second secret sequence comprises a sequence of bits that correspond to the bits of the configuration data sequence, and wherein the bits of the second secret sequence that correspond to the bits of the configuration data sequence that are encrypted have identical values to the corresponding bits of the configuration data sequence, for example (see column 8, line 29 through column 9, line 25). **Richards** discloses partially encrypted data that include plaintext and ciphertext, and discloses that the KTU ciphertext correspond to the KTU plaintext, thus the bits of the plaintext correspond to the configuration data sequence and the ciphertext correspond to the key/keys used. It is obvious to one skilled in the art of cryptography that bits of a second sequence that correspond to the bits of the

configuration data sequence that are encrypted may have identical values to the corresponding bits of the configuration data sequence.

As per claims 8 and 23, Richards discloses the claimed method of claim 7, wherein the decrypting step further comprises the step of: overwriting the bits in the partially-encrypted configuration data sequence using the bits of the second secret sequence that correspond to the bits of the first secret sequence that indicate which bits of the configuration data sequence are encrypted, for example (see column 7, lines 15-31 and column 8, line 40 through column 9). Not explicitly disclosed overwriting the bits. **Richards** discloses decrypting and recovering the entire application and discloses applying any known DES algorithm. Substitution cipher is well known in the art. It is obvious to one skilled in the art of cryptography that the overwriting step can be interpreted as a substitution cipher and overwriting the bits in the partially-encrypted configuration data sequence using the bits of the second secret sequence that correspond to the bits of the first secret sequence that indicate which bits of the configuration data sequence are encrypted does not depart from the spirit and scope of the invention disclosed by **Richards**.

As per claims 11 and 26, Richards discloses the claimed method of claim 1, wherein the decryption information comprises a list of bit positions within the configuration data sequence that are encrypted, for example (see column 7, lines 15-31 and column 8, line 40 through column 9, line 25).

As per claims 12 and 27, Richards discloses the claimed method of claim 1, wherein the decryption information comprises a list of ordered pairs, each ordered pair including a first value that indicates a bit position in the partially encrypted configuration data sequence that is encrypted, and a second value that corresponds to an unencrypted value for the bit position from the configuration data sequence, for example (see column 8, line 40 through column 9). **Richards** does not disclosed grouping the decryption information in a list of ordered pair, but discloses using any numbered of field. Claims 12 and 27 recite similar limitation as the rejected claims 7 and 22, and therefore are rejected on the same rationale as the rejection of claims 7 and 22.

As per claims 13 and 28, Richards discloses the claimed method of claim 1, wherein the decryption information comprises a list of ordered tuples, each ordered tuple including a first element that indicates a bit position in the partially encrypted configuration data sequence that is encrypted, for example (see column 7, lines 15-31 and column 8, line 40 through column 9), also discloses algorithm identifier that indicates which algorithm to use, for example (see column 7, lines 15-31 and column 8, line 40 through column 9) that meets the recitation of a second element that indicates whether the bit of the partially-encrypted configuration data sequence at the indicated bit position is to be modified or overwritten, and a third element that corresponds to an unencrypted value for the bit position from the configuration data sequence, for example (see column 7, lines 15-31 and column 8, line 40 through column 9).

As per claims 14 and 29, Richards discloses the claimed method of claim 13. **Richards** also discloses determining which data is to be modified or toggled using the identifier as mentioned in claims 4 and 18 above and discloses which data is to be overwritten using identifiers and decryption information as discussed in claims 10 and 23 above. It is obvious to one skilled in the art that the invention disclosed by **Richards** is capable of determining whether the bit of the partially-encrypted configuration data sequence identified by the first element is to be overwritten or modified by examining the second element of the tuple; if the bit is to be modified, then toggling the value of the bit at the identified bit position in the partially-encrypted configuration data sequence; and if the bit is to be overwritten, then overwriting the bit at the identified bit position in the partially-encrypted configuration data sequence using the value in the third element of the tuple.

As per claim 20, Richards discloses the claimed apparatus of claim 19, wherein the set of logic values are stored in the decryption memory store, for example (see column 11 and column 7, lines 45-67).

As per claim 21, Richards discloses the claimed apparatus of claim 19, apparatus of claim 19, wherein the set of logic values are stored in a memory store that is separate from the decryption memory store, for example (see column 11 and column 7, lines 45-67). It is also a design choice as to where to store the logic values.

As per claim 32, Richards discloses the claimed apparatus of claim 30, wherein the interface includes a plurality of input/output peripheral cells for interfacing between internal elements of the FPGA and a plurality of external circuits, for example (see column 11, line 45 through column 12, line 27 and column 1, lines 20-35).

As per claim 33, Richards discloses the claimed apparatus of claim 30, wherein the FPGA includes: a plurality of input/output peripheral cells for interfacing between the FPGA and a plurality of external circuits column 11, line 45 through column 12, line 27 and column 1, lines 20-35; user-configurable logic blocks for performing logical functions as defined by a user of the FPGA, for example (see column 11, line 45 through column 12, line 27 and column 1, lines 20-35 and column 4); interconnect elements for connecting the user-configurable logic blocks to the plurality of input/output peripheral cells, for example (see column 11, line 45 through column 12, line 27 and column 1, lines 20-35 and column 4); wherein the interconnect elements are configured using the configuration data sequence, for example (see column 11, line 45 through column 12, line 27 and column 1, lines 20-35 and column 4).

As per claims 34-35, Richards discloses the claimed apparatus of claim 30, wherein the decryption memory store is an SRAM memory and wherein the decryption memory store is a ROM, for example (see column 11, line 21 through column 12, line 27 and column 1, lines 20-35).

6. **Claims 9-10 and 24-25** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,385,723 to **Richards** in view of US Patent 6,223,290 to **Larsen et al.**.

6.1 **As per claims 9, 10, 24, and 25, Richards** substantially teaches the claimed method of claim 1, and further discloses loading configuring and processing an application in the IC card that meets the recitation of programming the memory cells (see column 4). **Richards** also discloses means of setting information corresponding to encrypted data and the logic values set in the selected memory cells correspond to the actual logic values of the configuration data sequence, for example (see column 7, lines 15-31 and column 8, line 40 through column 9) that meets the recitation of programming selected memory cells of the programmable memory device so as to set the logical values stored in the selected memory cells wherein the selected memory cells correspond to the bits of the configuration data sequence that are encrypted and the logic values set in the selected memory cells correspond to the actual logic values of the configuration data sequence. **Richards** further teaches in the background (columns 1-2) that programmable device can be one-time programmed by manufacture. The invention discloses how to secure such device to make it programmable multiple times. **Richards** does not explicitly disclose providing a one-time programmable memory device within the programmable device. However, **Larsen et al.** in an analogous art teaches programming a unique code into a memory of a programmable device so that the memory is permanently locked out and no further changes are allowed to the values stored, (see for example columns 6-7 and abstract). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Richards** to provide a one-time programmable memory device within the

programmable device and programming selected memory cells of the one-time programmable memory device so as to permanently set the logical values stored in the selected memory cells wherein the selected memory cells correspond to the bits of the configuration data sequence that are encrypted and the logic values set in the selected memory cells correspond to the actual logic values of the configuration data sequence as taught by **Larsen et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Larsen et al.** so as to the memory is permanently locked out and no further changes are allowed to the values stored.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses method and apparatus for securing transfer of data into a programmable logic device. Many of the claimed features, i.e. decrypting information that includes bit position and contains unencrypted and encrypted values, overwriting, key storage, etc. are disclosed in this reference.

US Patents:	5,915,017	Sung et al.
	6,378,071	Sasaki et al.
	6,654,889	Trimberger
	5,199,073	Scott
	6,118,869	Kelem et al.

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin

Patent Examiner

May 14, 2004

Emmanuel L. Moise

EMMANUEL L. MOISE
PRIMARY EXAMINER

4/11/2130